UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,699	06/13/2001	Richard J. Takahashi	052-0003	4290

29974 7590 02/24/2005

GAMMAGE & BURNHAM, PLC
c/o PortfolioIP
P.O. BOX 52050
Minneapolis, MN 55402

EXAMINER	
AKPATI, ODAICHE T	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 02/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/880,699	TAKAHASHI, RICHARD J.	
	Examiner	Art Unit	
	Tracey Akpati	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-42 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-42 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 06 March 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 3 received.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-13 are rejected under 35 U.S.C. 101 because it claims process steps that are not applied onto any hardware. Claim limitation showing software process steps without any application to a hardware device is not statutory.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-25 and 37-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sherigar et al (A Pipelined Parallel Processor to Implement MD4 Message Digest Algorithm on Xilinx FPGA).

With respect to Claim 1, the limitation of "a method for creating a message digest from a message, wherein a sequence of input words is derived from the message" is met on page 394, column 1, first paragraph; and "performing a portion of an operation, wherein the operation is a set of processes that operates on a word of the sequence; performing a portion of a next operation in parallel with performing the portion of the operation, wherein the next operation is a set of processes that operates on a next word of the sequence; and repeating performing the portion of

the operation and performing the portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence" is met on page 395, column 1 and 2. Sherigar et al does not explicitly disclose performing a portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence. However page 395, column 2, third paragraph states that a partial result of the operations are stored in external RAM for further processing in the final round.

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform a portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence so as to allow for each round of the process to execute so as to retrieve the final output.

With respect to Claim 2, the limitation of "performing a non-linear function on three of four variables stored in three of four registers" is met on page 395, column 1, last paragraph; and "adding an output of the non-linear function to the word, a constant word, and a fourth variable of the four variables, resulting in a first sum" is met on page 395, column 2, first paragraph and on column 1, third paragraph; and "circularly shifting the first sum by a number of bits, resulting in a shifted result; addingthe shifted result to contents of one of the four registers, resulting in a second sum; and replacing contents of one of the four registers with the second sum" is met on page 395, column 2, paragraphs 1-3.

With respect to Claim 3, the limitation of "temporarily storing the second sum, resulting in a stored sum, and wherein replacing the contents of one of the four registers comprises

replacing the contents with the stored sum" is met on page 397, section 3.2 and on page 398, section 3.3-3.5.

With respect to Claim 4, the limitation of "performing a non-linear function on three of four variables; and addingtogether the next word, a constant word, and a fourth variable of the four variables, resulting in a first sum" is met on page 395, column 1, last two paragraphs.

With respect to Claim 5, the limitation of "performing remaining processes of the next operation after performing the portion of the next operation" is met on page 395, column 2, paragraph 1.

With respect to Claim 6, the limitation of "addingan output of the non-linear function to the first sum, resulting in a second sum; circularly shifting the second sum by a number of bits, resulting in a shifted result; and adding the shifted result to one of the four variables" is met on page 395, column 2, paragraphs 1-3.

With respect to Claim 7, the limitation of "performing a second portion of the operation before performing the portion of the operation" is met on Fig. 1 and on page 395, column 1, third paragraph.

With respect to Claim 8, the limitation of "performing a non-linear function on three of four variables stored in three of four registers; and adding an output of the non-linear function. to

the word, a constant word, and a fourth variable of the four variables, resulting in a first sum" is met on page 395, column 1, last two paragraphs.

With respect to Claim 9, the limitation of "circularly shifting the first sum by a number of bits, resulting in a shifted result; adding the shifted result to contents of one of the four registers, resulting in a second sum; and replacing contents of one of the four registers with the second sum" is met on Fig. 3; page 395, column 2 and on page 396.

With respect to Claim 10, the limitation of "wherein performing the portion of the operation and performing the portion of the next operation are completed during a first clock cycle, and the method further comprises performing remaining processes of the next operation during a next clock cycle" is met on Fig. 3 and on page 395 and 396, section 2.2. The timing signals represent the use of a clock cycle.

With respect to Claim 11, the limitation of "performing a second portion of the operation during a preceding clock cycle" is met on page 398, section 3.3.

With respect to Claim 12, the limitation of "wherein the message comprises one or more 512-bitblocks, each of which includes sixteen 32-bit words, and the message digest includes 128 bits" is met in the abstract of page 394.

With respect to Claim 13, the limitation of "wherein the message digest is identical to

another message digest computed by MD5, given a same message" is met in the abstract of page 394. MD4 has the same basic structure as MD5. MD5 simply improves upon MD4's disadvantages.

With respect to Claim 14, its limitation is similar to Claim 1 limitation and hence its rejection can be found therein.

With respect to Claim 15, its limitation is similar to Claim 2 limitation and hence its rejection can be found therein.

With respect to Claim 16, its limitation is similar to Claim 4 limitation and hence its rejection can be found therein.

With respect to Claim 17, its limitation is similar to Claim 5 limitation and hence its rejection can be found therein.

With respect to Claim 18, its limitation is similar to Claim 6 limitation and hence its rejection can be found therein.

With respect to Claim 19, its limitation is similar to Claim 7 limitation and hence its rejection can be found therein.

With respect to Claim 20, its limitation is similar to Claim 8 limitation and hence its rejection can be found therein.

With respect to Claim 21, its limitation is similar to Claim 9 limitation and hence its rejection can be found therein.

With respect to Claim 22, its limitation is similar to Claim 10 limitation and hence its rejection can be found therein.

With respect to Claim 23, its limitation is similar to Claim 11 limitation and hence its rejection can be found therein.

With respect to Claim 24, its limitation is similar to Claim 12 limitation and hence its rejection can be found therein.

With respect to Claim 25, its limitation is similar to Claim 13 limitation and hence its rejection can be found therein.

With respect to Claim 37, the limitation of "an integrated circuit, which creates a message digest from a message, wherein a sequence of input words is derived from the message, and the message digest is created by performing a portion of an operation, wherein the operation is a set of processes that operates on a word of the sequence, performing a portion of a next operation

in parallel with performing the portion of the operation, wherein the next operation is a set of processes that operates on a next word of the sequence, and repeating performing the portion of the operation and performing the portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence" is met on page 394, column 1, first paragraph; and on page 395, columns 1 and 2. Sherigar et al does not explicitly disclose performing a portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence. However page 395, column 2, third paragraph states that a partial result of the operations are stored in external RAM for further processing in the final round.

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform a portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence so as to allow for each round of the process to execute so as to retrieve the final output.

With respect to Claim 38, the limitation of "a computer readable medium, coupled to the integrated circuit, which has computer executable instructions stored thereon that cause the processor to perform the portion of the operation, perform the portion of the next operation, and repeat performing" is met on page 395.

With respect to Claim 39, the limitation of "a first logic block, which performs the portion of the operation during a clock cycle, performs the portion of the next operation during the clock cycle, and repeats performing the portion of the operation and performing the portion of the next

operation until processes have been performed that sequentially operate on all remaining words of the sequence" is met on page 395.

With respect to Claim 40, the limitation of "a second logic block, coupled to the first logic block, which performs a second portion of the operation during a preceding clock cycle" is met on page 398.

With respect to Claim 41, the limitation of "an external interface, which transmits the message digest" is met on Fig. 1.

With respect to Claim 42, the limitation of "an external interface, which transmits data that was generated from the message digest" is met on Fig. 1.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 26-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Sherigar.

With respect to Claim 26, the limitation of "a first logic block which performs a portion of an operation during a clock cycle, wherein the operation is a set of processes that operates on a

word of the sequence, performs a portion of a next operation during the clock cycle, wherein the next operation is a set of processes that operates on a next word of the sequence, and repeats performing the portion of the operation and performing the portion of the next operation until processes have been performed that sequentially operate on all remaining words of the sequence" is met on page 395, column 1 and 2 and on Fig. 1 and 2; and "wherein additional passes through the first logic block are made until calculations have been performed that sequentially operate on all remaining words of the sequence" is met on page 397, column 2.

With respect to Claim 27, the limitation of "a non-linear function block, which receives three of four variables" is met on page 395, column 1, last paragraph; and "one or more first adders, which add together the next word, a constant word, and a fourth variable of the four variables, resulting in a first sum" is met on page 395, column 2, first paragraph; and on column 1, third paragraph; and "a second adder, which adds an output of the non-linear function block to the first sum, resulting in a second sum; a shifter, coupled to the second adder, which circularly shifts the second sum by a number of bits, resulting in a shifted result; and a third adder, coupled to the shifter, which adds the shifted result to one of the four variables" is met on page 395, section 2.1.

With respect to Claim 28, the limitation of "a multiplexer, coupled to the second adder, which passes the output of the non-linear function and the first sum to the second adder" is met on Fig. 1.

With respect to Claim 29, the limitation of "a second logic block, coupled to the first logic block, which performs a second portion of the operation during a preceding clock cycle" is met on Fig. 1 and 3.

With respect to Claim 30, the limitation of "a non-linear function block, which receives three of four variables stored in three of four registers" is met on page 395, column 1; and "one or more first adders, coupled to the non-linear function block, which add an output of the non-linear function block to the word, a constant word, and a fourth variable of the four variables, resulting in a first sum" is met on Fig. 1 and on page 395, column 1.

With respect to Claim 31, its limitation is similar to Claim 12 limitation and hence its rejection can be found therein.

With respect to Claim 32 and 36, its limitation is similar to Claim 13 limitation and hence its rejection can be found therein.

With respect to Claim 33, the limitation of "a frontcomputation logic block, which performs a portion of a first operation within a round of multiple operations during one or more clock cycles, wherein the first operation is a set of processes that operates on a word of the sequence" is met on Fig. 1 and page 395, column 1; and "a systolic computation logic block, coupled to the front computation logic block, which performs a second portion of the first operation during one or more subsequent clock cycles, and performs a portion of a next operation

during the one or more subsequent clock cycles, wherein the next operation is a set of processes that operates on a next word of the sequence, and the systolic computation block iterates until remaining operations within the round of multiple operations are completed" is met on page 395, column 2.

With respect to Claim 34, the limitation of "a non-linear function block, which receives three of four variables stored in three of four registers" is met on page 395, column 1, last paragraph; and "one or more first adders, coupled to the non-linear function block, which add an output of the non-linear function block to the word, a constant word, and a fourth variable of the four variables, resulting in a first sum" is met on page 395, column 2, first paragraph and on column 1, third paragraph.

With respect to Claim 35 its limitation is similar to Claim 27 limitation and hence its rejection can be found therein.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 571-272-3846. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

OTA

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100